

# Polityka Bezpieczeństwa jako kluczowy element tworzenia systemu informatycznego

Krzysztof Młynarski, Jacek Piechota  
Centrum Bezpieczeństwa Sieciowego S.A.  
e-mail: prezes@cbs.pl, jp@cbs.pl

**Abstrakt:** Autorzy przedstawiają całość procesu opracowywania Polityki Bezpieczeństwa dla typowego systemu informatycznego. Proces tworzenia Polityki Bezpieczeństwa jest zaprezentowany systematycznie - od zdefiniowania podstawowych pojęć, poprzez omówienie całości procesu opracowywania Polityki Bezpieczeństwa ze szczególnym zwróceniem uwagi na zagrożenia występujące we współczesnych systemach informatycznych, aż do wskazania i krótkiego omówienia dostępnej w sieci Internet dokumentacji źródłowej dotyczącej poruszanej tematyki.

## 1. Wprowadzenie

Polityka Bezpieczeństwa to zbiór precyzyjnych reguł rządzących zachowaniem osób mających dostęp do informacji przetwarzanych na terenie korporacji, jak i poza nią. Najważniejszym celem Polityki Bezpieczeństwa jest zapewnienie integralności systemu informatycznego wraz z przechowywanymi i przetwarzanymi w nim informacjami.

Najczęściej pod pojęciem systemu informatycznego rozumiemy sieć, lub sieci komputerowe ze wszystkimi komponentami typowymi dla tego rodzaju instalacji – serwerami, routerami, stacjami roboczymi itd. Okazuje się, iż z punktu widzenia Polityki Bezpieczeństwa takie rozumowanie jest błędne!

System informatyczny należy raczej zdefiniować jako całość systemu przetwarzania danych w przedsiębiorstwie – natomiast to, czym przetwarzamy te dane jest dla nas mniej istotne w początkowym okresie opracowywania Polityki Bezpieczeństwa. O systemie informatycznym możemy – paradoksalnie – mówić nawet w przypadku firmy czy też instytucji nie posiadającej ani jednego komputera. Ze względów bezpieczeństwa ważne jest jedynie to, czy jakiegokolwiek istotne informacje są w danej organizacji przetwarzane.

W krajach rozwiniętych opracowanie Polityki Bezpieczeństwa jest bardzo często warunkiem przekazania systemu informatycznego do eksploatacji. U nas Polityka Bezpieczeństwa nadal bywa lekceważona pomimo, iż w rzeczywistości powinna ona stanowić podstawę wszelkich działań zmierzających do stworzenia bezpiecznego systemu informatycznego. Obecnie nawet w Polsce istnieje bardzo wiele przedsiębiorstw, w których praktycznie całość obiegu informacji związana jest z wykorzystywaniem infrastruktury informatycznej. Rzadko kiedy zadajemy sobie pytanie, czy aby na pewno zapewniliśmy należyty poziom bezpieczeństwa własnego systemu informatycznego, który stanowi podstawę funkcjonowania naszej firmy?

Według badań przeprowadzonych przez amerykańskich ekspertów z zakresu bezpieczeństwa danych i systemów komputerowych (raport *Datapro* z roku 2000) ponad 80% zagrożeń w systemie informatycznym generują jego legalni użytkownicy. Popularni w mediach “hackerzy”, “crackerzy”, “cyber-anarchiści” i szpiedzy przemysłowi razem wzięci, generują zaledwie nieco ponad 7% istniejących zagrożeń. Resztę stanowią zagrożenia o charakterze losowym (pożar, powódź, awarie sprzętu i błędy oprogramowania), lub nie sklasyfikowanym jako przestępstwa czysto informatyczne – czyli np. zwykła kradzież sprzętu komputerowego lub okablowania.

Co bardziej zaskakujące – z badań tych wynika, że nie zawsze nakłady poniesione na zabezpieczenia logiczne i fizyczne wpływają na rzeczywisty poziom bezpieczeństwa naszych danych – w każdym przypadku najważniejszy okazuje się czynnik ludzki. Właśnie ze względu na

powyższe proporcje źródeł występujących zagrożeń tak istotnym elementem systemu bezpieczeństwa staje się Polityka Bezpieczeństwa.

## 2. Założenia przy tworzeniu Polityki Bezpieczeństwa

Zasady określone przez Politykę Bezpieczeństwa dotyczą całości procesu korzystania z informacji, niezależnie od sposobu jej gromadzenia i przetwarzania.

Zostały już opracowane dokumenty standaryzujące metody opracowywania, wdrażania i pielęgnacji Polityki Bezpieczeństwa. Do najważniejszych z nich należą obecnie:

- RFC 2196 "Site Security Handbook" [1],
- FIPS PUB 191 "Federal Information Processing Standards Publication 191 - Standard for: Guideline for the Analysis of Local Area Network Security" [2].

Powstaje coraz więcej publikacji fachowych opisujących metody tworzenia jednolitego systemu bezpieczeństwa [3], których autorzy doradzają rozpoczynanie tego żmudnego procesu od opracowania Polityki Bezpieczeństwa i dopasowania do jej zaleceń pozostałych elementów bezpieczeństwa – takich, jak wspomniane już zabezpieczenia logiczne i fizyczne.

Akceptacja i zrozumienie potrzeby opracowania Polityki Bezpieczeństwa przez kierownictwo instytucji ma kluczowe znaczenie dla powodzenia całego procesu realizacji przez organizację Polityki Bezpieczeństwa. Na początku procesu opracowania Polityki Bezpieczeństwa istotne jest wyznaczenie osoby zarządzającej całokształtem działań związanych z zapewnianiem systemowi wymaganego poziomu bezpieczeństwa, tzw. Oficera Bezpieczeństwa. Powinien to być specjalista informatyk bezpośrednio odpowiedzialny za ochronę danych przetwarzanych w systemie informatycznym.

Jednakże nie powinien to być administrator sieci lub któregokolwiek z jej elementów. W przeciwnym przypadku osoba taka mogłaby sama stanowić zagrożenie dla bezpieczeństwa systemu informatycznego (np. poprzez próbę tuszowania własnych błędów w administracji systemami sieciowymi).

## 3. Etapy tworzenia Polityki Bezpieczeństwa

Poniżej przedstawiamy standardowe etapy opracowywania i wdrażania Polityki Bezpieczeństwa. Jeszcze raz podkreślamy, że mianem "systemu informatycznego" określamy całość urządzeń, oprogramowania i mediów używanych do przetwarzania, przechowywania i przenoszenia informacji na terenie przedsiębiorstwa, a w tym także nośniki i media nie związane bezpośrednio z przetwarzaniem elektronicznym.

### 3.1. Wstępna ocena wartości informacji przetwarzanych w systemie informatycznym

Jest to podstawowy etap tworzenia Polityki Bezpieczeństwa. W ramach jego realizacji, tworzona jest baza danych zawierająca informacje dotyczące rodzajów informacji przetwarzanych w systemie informatycznym oraz aplikacji i sprzętu używanych do ich przetwarzania.

Zebrane podczas realizacji tego etapu informacje stanowią materiał do realizacji następnych etapów opracowywania Polityki Bezpieczeństwa.

### 3.2. Sklasyfikowanie wartości gromadzonych i przetwarzanych informacji

Informacje zebrane w pierwszym etapie są następnie klasyfikowane pod względem ich wartości dla przedsiębiorstwa. Kryteria brane pod uwagę, to m.in.: ogólny stopień poufności, możliwe do

przewidzenia skutki przedostatnia się danej informacji w ręce osób niepowołanych, skutki utraty lub modyfikacji danej informacji.

W wyniku przeprowadzonej analizy informacje przetwarzane w systemie informatycznym przedsiębiorstwa są dzielone na następujące klasy:

- Niesklasyfikowane (publikowane)
- Niesklasyfikowane (niepublikowane)
- Sklasyfikowane
- Poufne
- Tajne

Pomimo, iż szacowanie wartości informacji jest ryzykowne, jest ono niezbędnym etapem w procesie tworzenia systemu jednolitej ochrony danych.

### **3.3. Określenie prawidłowych kierunków przepływu informacji na terenie firmy oraz poza nią**

Posiadając niezbędne dane o rodzajach przetwarzanych w systemie informatycznym informacji, musimy przeanalizować kierunki przepływu informacji. W wyniku przeprowadzonej analizy powstaje Schemat Przepływu Informacji, który pozwala na wychwycenie słabych punktów w obiegu informacyjnym.

W wyniku przeprowadzenia tej analizy możemy podzielić system informatyczny na domeny ze wskazaniem kierunków przepływu informacji.

### **3.4. Analiza ryzyka**

Analiza ryzyka, czyli usystematyzowanie w postaci podziału na kategorie zagrożeń wraz ze środkami im przeciwdziałającymi. W wyniku takiej klasyfikacji jesteśmy w stanie opracować plan działania, który pozwoli na skierowanie większości środków na przeciwdziałanie najbardziej prawdopodobnym zagrożeniom.

Proponujemy przeprowadzenie analizy ryzyka z równoczesnym przypisaniem odpowiednich priorytetów różnym zagrożeniom mogącym mieć wpływ na działanie systemu informatycznego w firmie. W wyniku przeprowadzenia analizy ryzyka powinna powstać odpowiednia dokumentacja w formie formularza analizy ryzyka.

Formularz analizy ryzyka zawiera następujące informacje:

- opis ryzyka,
- potencjalny skutek,
- szacunkowy koszt eliminacji skutków,
- prawdopodobieństwo wystąpienia,
- względny priorytet,
- opis działań zapobiegawczych,
- koszt zabezpieczeń.

### **3.5. Opracowanie metodyki ochrony informacji dostosowanej do specyfiki systemu informatycznego firmy.**

Realizację tego etapu rozpoczynamy poprzez zdefiniowanie trzech, głównych poziomów ochrony:

- poziomu proceduralnego,
- poziomu fizycznego,
- poziomu logicznego.

Realizacja metodyki bezpieczeństwa na każdym z wymienionych poziomów realizowana jest przy wykorzystaniu odpowiednich środków bezpieczeństwa: fizycznych, technicznych i prawnych.

### **3.6. Opracowanie Polisy Bezpieczeństwa**

Opracowanie Polisy Bezpieczeństwa, czyli zbioru dokumentów formalnej podstawy przyjętej przez firmę Polityki Bezpieczeństwa. Polisa Bezpieczeństwa oprócz części ogólnej, zawierającej normy dotyczące metod bezpiecznego użytkowania systemu informatycznego powinna zawierać również dokumenty opracowane dla poszczególnych użytkowników, bądź też grup użytkowników, opracowane pod kątem konkretnych zadań wykonywanych przez te osoby. Każdy pracownik powinien potwierdzić znajomość Polisy Bezpieczeństwa własnoręcznym podpisem.

Dobrze skonstruowana Polisa Bezpieczeństwa pełni trzy podstawowe funkcje:

- zbioru przepisów obowiązujących każdego pracownika firmy,
- dokumentacji instruktażowej, która może być wykorzystywana przez pracownika jako źródło wiedzy o prawidłowych metodach wykonywania poszczególnych procedur związanych z pracą w systemie informatycznym.
- stanowi bezpośrednią podstawę wdrożenia całości Polityki Bezpieczeństwa w firmie.

### **3.7. Wdrożenie Polityki Bezpieczeństwa**

Wdrożenie Polityki Bezpieczeństwa - można podzielić na dwa podstawowe tory działania:

1. Instalację sprzętu i oprogramowania niezbędnego do utrzymania odpowiednio wysokiego poziomu fizycznego bezpieczeństwa danych przetwarzanych i przechowywanych w systemie informatycznym. Należy przeprowadzić analizę rynku pod kątem najlepszych dostępnych rozwiązań z zakresu sprzętu jak i oprogramowania.
2. Szkolenie przyszłych użytkowników systemu informatycznego wykorzystującego nowy system zabezpieczeń. Użytkownicy systemu informatycznego powinni zostać przeszkoleni zarówno w zakresie ogólnych zasad bezpieczeństwa systemu informatycznego, jak i prawidłowej obsługi konkretnych rozwiązań wykorzystywanych w codziennej pracy. Szkolenia mogą być prowadzone z wykorzystaniem sprzętu i oprogramowania, które później będzie wykorzystywane w codziennej pracy przeszkolonego personelu.

### **3.8. Rozwój i pielęgnacja Polityki Bezpieczeństwa**

Rozwój i pielęgnacja Polityki Bezpieczeństwa jest pracą o charakterze ciągłym. W miarę upływu czasu pojawiają się nowe zagrożenia oraz dokonywane są zmiany w systemie informatycznym (wymiana sprzętu czy też oprogramowania, wprowadzanie nowych rozwiązań, rotacja pracowników). Polityka Bezpieczeństwa musi stale uwzględniać nowe warunki - w przeciwnym przypadku staje się bezużyteczna.

## **4. Uwagi końcowe - czas i koszty**

Zasadniczym problemem przed podjęciem decyzji o stworzeniu i wdrożeniu Polityki Bezpieczeństwa w danej organizacji jest udzielenie odpowiedzi na pytania o czas potrzebny na realizację czynności związanych z opracowywaniem Polityki Bezpieczeństwa, oraz szacunkowe koszty przedsięwzięcia.

Na opracowanie Polityki Bezpieczeństwa składa się szereg czynności. Tylko w przypadku niektórych z nich daje się wstępnie określić czas niezbędny do ich realizacji, i tak:

- z naszych doświadczeń wynika, że czas potrzebny na przeprowadzenie audytu stanowiska roboczego PC wraz z wywiadem przeprowadzonym z użytkownikiem danego stanowiska roboczego wynosi od 60 do 90 minut/stanowisko,
- audyt serwera wraz z przeprowadzeniem wywiadu z jego administratorem trwa nie mniej niż 8 godzin roboczych.

Czas potrzebny na przeprowadzenie wszystkich innych czynności jest wprost uzależniony od:

- wielkości systemu informatycznego jako całości,
- różnorodności stosowanych w systemie informatycznym rozwiązań,
- ilości poszczególnych rodzajów informacji przetwarzanych w systemie informatycznym,
- środowiska pracy systemu informatycznego (poziom wymagań w zakresie bezpieczeństwa, typy użytkowników uprawnionych do korzystania z systemu, topologia systemu informatycznego itd.),

## 5. Zakończenie

Decydując się na opracowanie i wdrożenie Polityki Bezpieczeństwa powinniśmy opierać się na wiedzy i doświadczeniu fachowców na co dzień trudniących się zagadnieniami bezpieczeństwa systemów przetwarzania danych. Niewłaściwie opracowana Polityka Bezpieczeństwa nie spełni swojej funkcji, a wręcz – w skrajnych przypadkach – może okazać się elementem skutecznie utrudniającym lub wręcz uniemożliwiającym sprawne i bezpieczne przetwarzanie informacji wewnątrz organizacji.

Należy też pamiętać, że właściwie przeprowadzane audyty bezpieczeństwa mają kluczowe znaczenie w procesie analizowania zagrożeń, na jakie narażony jest system informatyczny. Ważne jest, aby audyty bezpieczeństwa były powtarzane – system informatyczny podlega stałym zmianom, co w efekcie prowadzi najczęściej do wyłaniania się nowych zagrożeń.

Bardzo istotnym elementem jest sam moment rozpoczęcia wdrażania Polityki Bezpieczeństwa. Należy pamiętać, że każdy system bezpieczeństwa nakłada na użytkowników szereg, nieraz uciążliwych ograniczeń. Dlatego też zdecydowanie odradzamy jednorazowe wprowadzenie wszystkich obostrzeń wynikających z opracowania Polityki Bezpieczeństwa w przedsiębiorstwie.

Dobrym i praktykowanym rozwiązaniem jest stopniowe wdrażanie Polityki Bezpieczeństwa wraz ze stopniowym podnoszeniem świadomości użytkowników w zakresie bezpieczeństwa danych i systemów komputerowych (przez udział we właściwie dobranych szkoleniach i seminariach). Nagłe wprowadzenie wielu obostrzeń bez uprzedzenia powoduje naturalny odruch buntu u wielu osób, co w efekcie prowadzi do zniechęcenia i mniej lub bardziej uświadomionych prób omijania wprowadzanych zasad postępowania.

Z drugiej jednak strony ważna jest stanowczość w egzekwowaniu zasad nałożonych przez Politykę Bezpieczeństwa – w przeciwnym przypadku zasady te szybko staną się jedynie martwym zbiorem przepisów i zaleceń ignorowanych przez większość pracowników.

## Bibliografia

1. <http://www.faqs.org/rfcs/rfc2196.html>
2. <http://www.itl.nist.gov/fipspubs/fip191.htm>
3. Polecamy ofertę dostępną na: <http://www.amazon.com>